Chapter 12

Information Technology Policy and Procedures

Approved by the Eastern Board of Regents December 05, 2025.

Last Revision June 2021

Table of Contents

12.001 – Technology Support Policy 4
Submitting a Request 4
12.002 – Computer Use Policy 4
Purpose and Scope 4
Computer Use Definitions 4
Computer Use Policy 5
Computer Use Procedures 7
Computer Abuse Investigation Procedures 8
Gramm-Leach Bliley Act (GLBA) 8
Family Educational Rights and Privacy Act (FERPA) 9
12.003 – Password Policy 9
Password Requirements 9
Multi-Factor Authentication (MFA) 10
Compliance 10
12.004 – Computer Virus and Malware Policy 10
Additional Information 11
12.005 – Clean Desk Policy 11
Procedures 11
12.006 – Use of Artificial Intelligence (AI) 12
Policy Statement 12
Academic Integrity 13
Privacy and Data Security 13
Bias and Fairness 13
Accountability 13
Procedures 13
Compliance and Enforcement 13
12.007 – Artificial Intelligence (AI) Policy 13
Data Privacy and Confidentiality 13
Legal Compliance and Intellectual Property 14
Security and Procurement 14
Transparency and Responsible Use 15
Usage of Smart Glasses 15
12.008 – College Email Acceptable Use Policy 16

Acceptable Use Includes 16
Unacceptable Use Includes, but is Not Limited To 16
Security and Privacy 16
Account Management 16
Enforcement 17
12.009 – Personal Device Usage 17
Risk of Using Employees Personal Devices 17
Shadow IT 17
Personal Use Verification 18
05.010 - Data Privacy 18
Definitions 18
Data Collection & Use 18
Sensitive Data Protection 19
Individual Rights Under OKDPA 19
Data Security 19
Third-Party Service Providers 19
Data Retention and Disposal 19
Data Breach Response 19
Compliance and Enforcement 20

12.001 – Technology Support Policy

This policy informs the Eastern Oklahoma State College (Eastern) community about the procedures and requirements for obtaining technical support for campus technology resources.

This policy applies to all technology resources owned, hosted, or supported by Eastern. Information Technology (IT) does not provide installation or maintenance support for hardware or software that has not been pre-approved by IT.

Submitting a Request

All technical support requests must be directed to the Information Technology Services.

Requests can be submitted via email, the Service Help Desk web portal, or by phone, as listed on the Eastern website.

When making a technical support request, please be mindful to submit your request in a timely manner to prevent unnecessary delays. Include the following details:

- Name, department, office location, and telephone extension of the person making the request.
- Detailed description of the problem, including any error messages or warnings.
- Location of the equipment needing service.
- Urgency of the request.

12.002 – Computer Use Policy

Purpose and Scope

Access to modern information technology is essential to the pursuit and achievement of excellence across the Eastern Oklahoma State College (Eastern) mission of instruction, research, and academic advancement. The privilege of using computing systems and software, as well as internal and external data networks, is important to all members of the Eastern community. The preservation of that privilege for the full community requires that each individual student, faculty member, staff member, and administrator comply with institutional and external standards for appropriate use. This policy will establish general guidelines for the use of Eastern computing standards for appropriate use and for the use of Eastern computing resources equipment, services, software, and computer accounts by students, faculty, staff, and administration.

Computer Use Definitions

Abuser – Any user or other person who engages in misuse of computing resources as defined in this policy.

Computing resources – Includes computers, computer equipment, computer assistance services, software, computer accounts provided by Eastern, information resources, electronic communication facilities (including electronic mail, telephone mail, internet access, network access), or systems with similar functions.

Computer account – The combination of a user number, username, or user id and a password that allows an individual access to a mainframe computer or some other shared computer or network.

Information resources – Data or information and the software and hardware that render data or information available to users.

Network – A group of computers and peripherals that share information electronically, typically connected to each other by either cable or satellite link.

Peripherals – Special-purpose devices attached to a computer or computer network, such as printers, scanners, plotters, and similar equipment.

Server – A computer that contains information shared by other computers on a network.

Software – Programs, data, or information stored on magnetic media (tapes, disks, diskettes, cassettes, etc.). Usually used to refer to computer programs.

System Administrator – Faculty, staff, or administrators employed by a central computing department such as Computer Services whose responsibilities include system, site, or network administration and other faculty, staff, or administrators whose duties include system, site, or network administration. System administrators perform functions including, but not limited to, installing hardware and software, managing a computer or network, and keeping a computer operational. System administrators include any person responsible for a system which provides the capability to assign accounts to other users.

User – Any individual who uses, logs in, attempts to use, or attempts to log into a system, whether by direct connection or across one or more networks, or who attempts to connect to or traverse a network, whether via hardware, software, or both. Each user is responsible for his/her use of the computer resources and for learning proper data management strategies.

Computer Use Policy

Appropriate Use of Computing Resources – The computing resources provided by Eastern are primarily intended for teaching, educational, research, administrative purposes, and may generally be used only for authorized Eastern-related activities. Use of the computing resources is governed by all applicable Eastern policies, including, but not limited to, sexual harassment, copyright, and student and employee disciplinary policies, as well as by applicable federal, state, and local regulations.

Prohibited Use of Computing Resources – Eastern characterizes misuse of computing and information resources and privileges as unethical and unacceptable. Misuse constitutes cause for taking disciplinary action. Misuse of computing resources includes, but is not limited to, the following:

- Attempting to modify, remove, or add computer equipment, software, or peripherals without proper authorization.

- Accessing computers, computer software, computer data or information, or networks without proper authorization, regardless of whether the computer, software, data, information, or network in question is owned by Eastern, including but not limited to, abuse, or misuse of networks to which Eastern belongs or computers at other sites connected to those networks.
- Circumventing or attempting to circumvent normal resource limits, logon procedures, and security regulations.
- Sending fraudulent computer mail, breaking into another user's electronic mailbox, or reading another user's electronic mail without proper permission.
- Sending any fraudulent electronic transmission including but not limited to fraudulent requests for confidential information, fraudulent submission of electronic purchase requisitions or vouchers, and fraudulent electronic authorization of purchase requisitions or vouchers.
- Violating any software license agreement or copyright, including copying or redistributing copyrighted computer software, data, or reports without proper, recorded authorization.
- Using Eastern computing resources to harass or threaten others.
- Using Eastern computing resources for development, posting, transmission of, or link to, any of the following: commercial or personal advertisements, solutions, promotions, destructive programs, political materials, messages which are fraudulent, harassing, obscene, indecent, profane, intimidating, or otherwise unlawful, or any other unauthorized or personal use.
- Taking advantage of another's naivete or negligence to gain access to any computer account, data, software, or file that does not belong to the user or for which the user has not received explicit authorization to access.
- Physically interfering with other users' access to the Eastern computing resources.
- Encroaching on others use of Eastern computer resources, including but not limited to, disrupting other users use of computer resources by excessive game playing, by sending electronic chain letters or other excessive messages, either locally or off-campus, printing excessive copies of documents, files, data or programs, modifying system facilities, operating systems, or disk partitions, attempting to crash or tie up an Eastern or network computer, or damaging or vandalizing Eastern or network computing resources, equipment, software, or computer files.
- Disclosing or removing proprietary information, software, printed output or magnetic media without the explicit permission of the owner.
- Reading other users' data, information, files, or programs on a display screen, as printed output, or via electronic means, without the owner's explicit permission.
- Violating any applicable federal, state, or local regulations.

User Responsibility – All users of Eastern computing resources must act responsibly. Every user is responsible for the integrity of these resources. All users of Eastern-owned or Eastern-leased computing resources must respect the rights of other computing users, respect the integrity of the physical facilities and controls, and respect all pertinent license and contractual agreements. It is the Eastern policy that all members of its community act in accordance with these responsibilities, relevant laws, and contractual obligations, and the highest standards of ethics.

Password Protection – Each user is responsible for maintaining absolute security of any password or password right granted to the user. Passwords must not be "shared' with another user. Password security helps to protect the Eastern system against unauthorized access.

Computing Resources Access – Access to Eastern's computing resources is a privilege granted to Eastern students, faculty, staff, and administrators. Eastern reserves the right to limit, restrict, or extend computing privileges and access to its information resources.

Freedom of Communication – It is the intention of Eastern to maximize freedom of communication for purposes that further the goals of Eastern. Eastern places high value on open communication of ideas, including those new and controversial.

General Right of Privacy – A general right of privacy should be extended to the extent possible to the electronic environment. Eastern and all electronic users should treat electronically stored information in individual files as confidential and private. Contents should be examined or disclosed only when authorized by the owner, approved by an appropriate institution official, or required by law. Privacy is mitigated by the following circumstances.

- Eastern is an agency of the State of Oklahoma and therefore subject to the Oklahoma Open Records Act. For Eastern employees, electronic information created in the performance of their duties may be public records, just as are paper records. Such records may be subject to review and/or release under Oklahoma law. All computer files and email communications, unless subject to a specific privilege, are subject to production under the Oklahoma Public Records Act and, when relevant, to discovery in civil litigation. In these cases, disclosure of personal email or files not related to the specific issue discussed in any Public Records request or discovery will be avoided to the extent allowed by law.
- Administrative files of Eastern are generated as part of the process of managing the institution. Files that employees create or maintain can be reviewed by supervisors within this administrative context. Generally, faculty research files and files relating to scholarly endeavors will not be subject to such a review.
- There is an acknowledged trade-off between the right of privacy of a user and the need of system administrators to gather necessary information to ensure the continued functioning of these resources. In the normal course of system administration, system administrators may monitor any computing activity or examine activities, files, electronic mail, and printer listings to gather sufficient information to diagnose and correct problems with system software or hardware. Sometimes system administrators may monitor computing activity or access files to determine if security violations have occurred or are occurring. In that event, the user should be notified as soon as practical. System administrators at all times have an obligation to maintain the privacy of a user's files, electronic mail, and activity logs.

Computer Use Procedures

Computer accounts will be issued to authorized users only by Computer Services personnel or their designee.

Prior to issuance of an account and password all users must execute such forms including an acknowledgement and acceptance of the terms of this policy, as may be reasonably required by Eastern.

User passwords must be kept private and may not be disclosed to any other individual or entity. A password must NEVER be posted or placed where it can be discovered by someone other than the user.

Each user will select a User id in accordance with rules established by Computer Services. The User id will be used consistently for all logons.

Personal passwords will be maintained by the individual user and must be changed at least every 180 days, or at more frequent intervals as the user may elect. Passwords shall be selected in accordance with the rules established by Computer Services. In the event another person learns a user's password, the user must immediately change the password.

Any user who learns of an unauthorized user of his/her account must report the unauthorized use to Computer Services immediately.

Computer Abuse Investigation Procedures

In the event it appears that a user has abused or is abusing his/her computing privileges, or engages in any misuse of computing resources, then Eastern may pursue any or all of the following steps to protect the user community.

- Take action to protect the system(s), user jobs, and user files from damage.
- Begin an investigation and notify the suspected abuser's project director, instructor, academic advisor, dean or administrative office of the investigation.
- Refer the matter for processing through the appropriate Eastern disciplinary system.
- Suspend or restrict the suspected abuser's computing privileges during the investigation and disciplinary processing. A user may appeal such a suspension or restriction and petition for reinstatement of computing privileges through the procedures existing at the time the user requests an appeal, which procedures will be provided to the appealing user in writing.
- Inspect the alleged abuser's files, diskettes, and/or tapes. System administrators must have reasonable cause to believe that the trail of evidence leads to the user's computing activities or computing files before inspecting any user's files.
- In the event the misuse also constitutes a violation of any applicable federal, state, or local law, Eastern will refer the matter to appropriate law enforcement authorities.

Gramm-Leach Bliley Act (GLBA)

The Gramm-Leach Bliley Act requires financial institutions to protect the privacy and security of consumers' nonpublic personal information. It requires that institutions:

- Implement measures to secure students' personal financial information.
- Inform students about how their data is collected, shared, and protected.

- Only share personal information with third parties under certain conditions and provide customers with the opportunity to opt-out in some cases.

Family Educational Rights and Privacy Act (FERPA)

The Family Educational Rights and Privacy Act is a federal law that protects the privacy of student educational records. It gives the student the following expectations:

- The right to inspect and review their educational records.
- The institution cannot release personally identifiable information from a student's record without written consent, except under certain conditions.

The right to request corrections to their records if they believe information is inaccurate or misleading.

12.003 – Password Policy

Passwords play a critical role in ensuring information security at Eastern Oklahoma State College, serving as the first line of defense for user accounts.

This policy applies to all employees, students, and any other individuals with access to an Eastern network, account, or system.

Password Requirements

The Information Technology Department manages password guidelines, which include the following:

- All user-level and system-level passwords must follow Eastern's password guidelines.
- Passwords for Eastern accounts must not be reused for personal accounts or other Eastern purposes.
- Administrator or system-level accounts must have a unique password that is different than other accounts held by the same user.
- Strong passwords are longer and more secure with additional characters.
- Eastern encourages the use of passphrases – passwords made up of multiple words, with numbers or symbols included.
- Passwords must not be shared with anyone, including supervisors, coworkers, or family. All passwords are treated as confidential Eastern information.
- Passwords must never be inserted into email messages.
- Users must not use the "Remember Password" feature in applications (e.g., web browsers) for Eastern accounts.
- Passwords must be changed if there is a reason to believe they have been compromised or when prompted by Eastern.
- If a user suspects that a password has been compromised, they must report the incident to Eastern Information Technology immediately.

Multi-Factor Authentication (MFA)
Whenever available, multi-factor authentication (MFA) is required to provide an additional layer of security.

Compliance
All Eastern users must comply with these password guidelines. Violations may result in restricted access, loss of privileges, or other actions, as determined by Eastern, to protect its accounts, networks, and systems.

12.004 – Computer Virus and Malware Policy

Eastern Oklahoma State College maintains the operational stability and efficiency of its IT systems by actively overseeing the activities and communications on campus network and affiliated devices. This encompasses monitoring both on-campus and off-campus originating traffic to safeguard the integrity of the College's IT infrastructure. The monitoring focuses on detecting computer viruses, malware, unauthorized system access attempts, system performance, and adherence to institutional policies. Eastern retains the authority to intercept and isolate any network traffic or computing resources that may jeopardize the security of the College's systems, data, or infrastructure. This includes, but is not limited to, files, messages, network communications, and connected devices.

Every device connecting to the campus network is required to have a current and active antivirus solution installed. The antivirus software should be configured to automatically clean or quarantine any infected file as necessary. Routine automatic updates for the antivirus software are mandatory. Scheduled virus scans on devices must occur without the need for manual intervention. In cases where this automated scanning is not feasible, users hold the responsibility of initiating scans regularly and updating the software to counteract emerging threats.

All computers issued by the College are obligated to employ the antivirus software provided and set up by the IT Services department. Modifying or disabling the installed antivirus software is prohibited unless explicitly authorized by Eastern IT Services.

The management of servers and network equipment for the campus is largely handled by Eastern Information Technology Services. Consequently, these IT Services oversee the antivirus systems on these systems. Interfering with, tampering, or circumventing the security and antivirus systems on equipment managed by Eastern IT Services is a breach of the College's acceptable use policy.

Should a computer system become infected with a virus or malicious software, actions such as blocking, quarantining, or removal from the College network may be implemented until a PC Technician or Systems Administrator confirms the system's virus-free status.

All incoming emails directed to the College are subjected to viruses, malware, and spam scans via Google. Emails posing potential risks are blocked. However, given that no security software is infallible, users must exercise prudent discretion when opening emails or attachments.

External websites known to be sources of computer viruses and malware are prohibited and blocked. Despite this measure, users should remain cautious when accessing external websites, as no security software can guarantee complete protection.

In the event of a widespread virus or malware attack, Eastern IT Services will promptly inform the College community through Broadcast emails and social media channels. Should the situation be necessitated, the College IT Services may initiate comprehensive system scans using the latest virus definitions. In certain cases, manual intervention may be requested, and affected individuals will be directed to seek assistance at PC Support Services in the Bill Hill Library/Administration Building.

Additional Information

All students, faculty, and employees of Eastern Oklahoma State College must actively minimize the risk of their desktop systems infecting other systems or shared server files. Despite taking precautionary measures, the rapid spread of malicious code through means such as email and shared files can still pose a risk. Thus, maintaining up-to-date antivirus software is critical.

Exercise caution and never open files or macros attached to emails from unfamiliar, suspicious, or untrusted sources. Similarly, if you receive an unexpected attachment from a known individual, refrain from opening it and delete the attachment immediately.

Dispose of spam, chain emails, and other unsolicited messages without forwarding them.

Abstain from downloading files from sources that are unknown or seem suspicious.

12.005 – Clean Desk Policy

Unsecure confidential or regulated materials pose a security risk to Eastern. A clean desk policy helps minimize information security vulnerabilities, ensures compliance with state law (62 O.S. § 34.32), and aligns with ISO 27001/17799 standards. This policy also supports the protection of individual privacy and reflects Eastern's commitment to responsible information management.

This policy applies to all Eastern employees, vendors, and partners, with access to Eastern's information resources. In addition to mitigating risks, it promotes a professional image by demonstrating a culture of accountability and respect for stakeholders.

Procedures

Confidential and regulated information, whether paper-based or electronic, must always remain secure and stay within the data custodian's office when not in use.

When assisting a student or employee, only relevant documents should be visible. Information unrelated to the current individual must remain concealed.

Workstation screens must be locked when leaving a workspace unattended.

Workstations must be shut down completely at the end of the workday.

Desktops must be cleared of confidential and regulated materials during any period of absence and at the end of the business day.

File cabinets containing confidential and regulated information must be closed and locked when not in use or when left unattended.

Keys to secured storage units must not be left unattended or accessible to unauthorized individuals.

Passwords must not be written on Post-it/sticky notes or stored in an accessible location.

Printed confidential and regulated materials must be retrieved immediately from printers or fax machines.

Documents containing confidential and regulated information must be shredded at the end of their retention period. They must never be discarded in regular waste bins or recycling bins.

USB drives or other digital storage devices containing confidential and regulated information must be stored in a locked drawer.

Time should be allocated to properly secure confidential and regulated information within the custodial department. Confidential paper documents should not be removed from the Eastern campus.

12.006 – Use of Artificial Intelligence (AI)

The purpose of this policy is to guide the responsible and ethical use of Artificial Intelligence (AI) technologies within the College environment. This policy ensures that the use of AI tools aligns with the College's mission, promotes academic integrity, protects privacy, and fosters trust among students, faculty, staff, and the community.

This guidance applies to all students, faculty, staff, who use AI tools or technologies within the College system. It covers all AI systems used for education, administration, and operations. This includes, but is not limited to, automated grading tools, generative AI, data analysis software, virtual assistants, and any third-party AI platforms integrated into the College's systems.

Policy Statement

Eastern encourages the innovative and ethical use of AI tools to enhance learning, streamline operations, and improve decision-making processes.

Transparency must be maintained when AI tools are used for instruction, advising, grading, or student engagement. Users must be informed if they are interacting with an AI system.

AI is one of the many technologies used on our campus, and its use will align with existing regulations to protect student privacy, ensure accessibility to those with disabilities, and protect

against harmful content. Faculty, staff, and students must not share personally identifiable information with consumer-based AI systems.

Academic Integrity
Academic integrity is essential. Students may use AI tools (such as chatbots or writing assistants) only when explicitly permitted by instructors and in accordance with course guidelines. Unauthorized use of AI tools to complete coursework is considered plagiarism or academic misconduct.

Privacy and Data Security
AI systems must comply with FERPA (Family Educational Rights and Privacy Act) and other relevant data protection laws. AI tools collecting or processing personal information must follow College data privacy policies.

Bias and Fairness
AI technologies should be reviewed periodically to ensure that they are free from biases and do not discriminate against any group of individuals based on race, gender, disability, or other protected characteristics.

Accountability
Faculty, staff, and administrators are responsible for ensuring that AI tools are used responsibly. Vendors providing AI services must meet the College's ethical and data security standards.

Procedures
Instructors must clearly indicate in their syllabi whether AI tools are permitted or restricted in coursework and assessments.

Students using AI tools with permission must cite the AI system in their work, like citing traditional sources, to maintain transparency.

Compliance and Enforcement
Violations of this policy, including unauthorized use of AI tools, will be handled in accordance with academic misconduct or employee disciplinary procedures, as applicable.

The College reserves the right to suspend or discontinue the use of any AI tool or service that fails to meet ethical, privacy, or security standards.

12.007 – Artificial Intelligence (AI) Policy

Data Privacy and Confidentiality
The paramount concern for all AI use at EOSC is the protection of sensitive institutional data, especially student and employee Personally Identifiable Information (PII).

Prohibition of Sensitive Data Upload: Students, faculty, and staff are strictly prohibited from inputting, uploading, or copying Restricted or Confidential Data into general-purpose, public AI

tools (e.g., free versions of large language models/LLMs) that do not have a formal, executed Data Protection Agreement (DPA) with EOSC.

- Restricted Data includes, but is not limited to: student PII protected by FERPA (grades, disciplinary records, ID numbers), employee records, financial aid information, and confidential research data.

Data Minimization and Anonymization: For any AI application, both in academic and administrative settings, the principle of data minimization must be applied. Only the minimum amount of data necessary should be used, and PII must be properly anonymized or de-identified before use in training or prompting AI models, unless explicit consent and a DPA are in place.

Data Ownership: All data generated, collected, or processed by an AI system in the course of college-related activities remains the property of Eastern Oklahoma State College or the original data owner (e.g., the student). AI vendors must not retain the right to use college data to train their commercial models unless explicitly agreed to in the contract.

Legal Compliance and Intellectual Property

All AI use must adhere to federal and state laws, as well as institutional intellectual property (IP) policies.

FERPA Compliance: Any AI system that collects, processes, or stores student education records must fully comply with the Family Educational Rights and Privacy Act (FERPA). This requires vendor contracts to specifically address FERPA compliance and prohibit the unauthorized disclosure or use of student PII.

Copyright and IP:

- Input (Training Data): Any AI model developed by or for EOSC must be trained on data acquired in a legally compliant manner, respecting all copyright and licensing agreements.

- Output (Generative Content): Users must be aware that the legal status of AI-generated content (e.g., text, images, code) is unsettled. Users are responsible for ensuring that the final submitted or published work does not infringe on the copyright of third parties, particularly when using AI to summarize or generate material based on external sources.

- Licensing Disclosure: When using AI-generated output in public research or administrative materials, the tool and its license must be explicitly disclosed.

Accessibility: AI tools adopted by EOSC must comply with all relevant accessibility standards (e.g., ADA, Section 508) to ensure equitable access for students and employees with disabilities.

Security and Procurement

The college's IT department (or relevant administrative office) must maintain oversight of all AI tools and vendors to manage institutional risk.

AI Tool Vetting and Risk Assessment:

- Mandatory Review: All proposed AI tools and third-party vendors, regardless of whether they are for academic, research, or administrative use, must undergo a formal IT risk assessment and security review before procurement or adoption.

- Risk Tiers: Tools should be classified based on risk (e.g., High, Medium, Low) according to the type of data they process and the sensitivity of the decisions they influence.

- High-Risk: AI used for critical institutional decisions (e.g., student retention prediction, financial aid assessment) requires the highest level of human oversight and continuous security auditing.

Security Controls: AI applications deployed on EOSC networks must adhere to the college's existing cybersecurity standards, including:

- Use of Multi-Factor Authentication (MFA).
- Regular security patching and vulnerability testing.
- Logging and auditing of all user and system access to AI tools, particularly those interacting with high-value data.

Incident Response: All employees must report suspected data breaches, security incidents, or AI misuse to the IT department immediately. The college must have a defined plan to respond to security incidents involving AI systems, including immediate notification to affected parties as required by law.

Transparency and Responsible Use

Model Transparency (for Internal Tools): When the college implements internal AI models for administrative purposes (e.g., student success analytics), there must be documentation on the data sources, the algorithm's logic, and the limitations of the model. Affected individuals (e.g., students) have the right to request a human review of any high-stakes decision made or influenced by an AI system.

Prohibition of Harmful Use: AI shall not be used to create or disseminate deepfakes, facilitate harassment, impersonation, discrimination, or any content that violates EOSC's Student Code of Conduct, Nondiscrimination Policy, or applicable law.

Usage of Smart Glasses

Due to institutional data privacy, cybersecurity, and student information protection requirements, the use of smart glasses is not permitted for official College business. These devices may capture or transmit audio, video, or other sensitive information in ways that cannot be adequately secured or monitored under current institutional technology standards. To protect confidential student and employee information and ensure compliance with applicable privacy regulations, employees should not use smart glasses while performing work-related duties.

12.008 – College Email Acceptable Use Policy

This policy establishes the acceptable use of college-issued email addresses and ensures the responsible use of electronic communication by all faculty, staff, and students. This policy applies to all individuals who are issued a college email address, including faculty, staff, students, contractors, and authorized affiliates.

College email accounts are provided to support academic, administrative, and operational functions. All users are expected to use these accounts in a responsible, ethical, and lawful manner consistent with the mission and policies of the college.

Acceptable Use Includes

- Communicating for official college business, including academic and administrative matters.
- Engaging in professional correspondence related to teaching, research, and college-related services.
- Participating in college-sponsored activities, events, and programs.
- Complying with federal, state, and institutional privacy and data protection laws (e.g., FERPA, HIPAA, etc.).

Unacceptable Use Includes, but is Not Limited To

- Using the college email for personal financial gain, political campaigning, or commercial activities unrelated to the college.
- Sending threatening, harassing, obscene, or discriminatory messages.
- Sharing login credentials or allowing unauthorized access to an account.
- Engaging in phishing, spamming, or any form of unauthorized mass communication.
- Transmitting confidential or sensitive college information without proper authorization or security.
- Automatically forwarding college email to personal accounts without appropriate safeguards.

Security and Privacy

Users are responsible for maintaining the security of their email accounts, including using strong passwords and reporting suspicious activity. While the college takes reasonable steps to ensure privacy, email communications may be monitored or accessed for legal, security, or administrative reasons. All emails (personal or private) sent through a college email address may be subject to the Oklahoma Open Records Act.

Account Management

- Email accounts for faculty and staff are deactivated upon separation from employment unless otherwise authorized.
- Student accounts may remain active for a defined period after graduation or withdrawal, as determined by the college's IT policy.
- All accounts are the property of the college and must be used in accordance with institutional policies.

Enforcement
Violation of this policy may result in disciplinary action, including but not limited to revocation of email privileges, suspension, termination, or legal action as appropriate.

12.009 – Personal Device Usage

The purpose of this policy is to establish clear guidelines prohibiting the use of personal computers, laptops, or other non-college-owned computing devices for any college-related work. This policy is designed to protect institutional data, maintain compliance with open records laws, safeguard against data loss, and minimize legal exposure for both the college and its employees.

All employees, contractors, and affiliated personnel are required to conduct college business exclusively on college-issued or college-managed devices. Under no circumstances should work-related files, documents, or communications be created, stored, or accessed on personal computers, laptops, or external media. All official work must be saved to a college-managed server, shared drive, or authorized cloud service where appropriate access, control, and retention policies are in place. This ensures that institutional records are preserved, accessible in the event of employee separation, and available for audits, open records requests, or legal investigations.

Risk of Using Employees Personal Devices
Using personal devices for college work introduces substantial risks, including potential loss of data, inability to retrieve records, and security vulnerabilities. In the event of an open records request or internal investigation, personal devices used for college work may be subject to legal hold, confiscation, or forensic examination. Employees should be aware that use of personal equipment for official duties may result in the permanent loss of personal data or devices if they are involved in a legal matter or compliance review.

Violations may result in disciplinary action, including loss of access to systems, revocation of technology privileges, or formal personnel review.

This policy will be reviewed and updated annually or as necessary in response to legal, regulatory, or operational changes. All employees are responsible for understanding and complying with this policy and should direct any questions or concerns to the college's IT or compliance office.

Shadow IT
The use of IT related hardware, software, or even services without the knowledge or approval of the IT department is called Shadow IT.

The main problems that result from Shadow IT:

- Security Risks: Unapproved tools often lack proper security protocols, making the organization vulnerable to data breaches and cyberattacks.
- Compliance Issues: Shadow IT can lead to non-compliance with regulations like GDPR or HIPAA, resulting in fines and legal penalties.

- Increased Costs: Employees might subscribe to services or purchase software without IT's knowledge, leading to duplicate or unused licenses and unnecessary expenses.
- Lack of Visibility and Control: IT departments lose visibility into what's happening on their networks and can't effectively manage or secure the tools being used.
- Reduced Efficiency: Shadow IT can lead to fragmented workflows, inconsistent data management, and difficulties in troubleshooting technical issues.

Personal Use Verification

In a case where an employee has used their personal computer, the computer is required to be cleaned by the Director of IT. Upon termination of the employee, all personal computer information will be given to the college. This may be the hard drive, stick drive, external hard drive, etc. A checklist system will be used by Human Resources at the time of exiting the college.

05.010 - Data Privacy

The purpose of this policy is to establish institutional standards and procedures to ensure compliance with the Oklahoma Data Privacy Act (SB 546) (OKDPA). This policy applies to all employees, contractors, vendors, volunteers, and third parties who collect, access, maintain, transmit, or otherwise process personal data on behalf of the College. It also applies to all institutional systems, devices, services, and platforms used to process personal data, whether owned by the College or provided through a third-party service provider.

The College is committed to safeguarding personal data and complying with the Oklahoma Data Privacy Act.

Definitions

Personal Data refers to any information that is linked or reasonably linkable to an identifiable individual. Sensitive Personal Data includes information such as Social Security numbers, driver's license or state identification numbers, financial account information, health-related information, biometric identifiers, student education records protected under FERPA, and authentication credentials such as usernames and passwords. Processing refers to any operation performed on personal data, including its collection, use, storage, disclosure, analysis, or deletion.

A Controller is the entity that determines the purpose and means of processing personal data, while a Processor is a third party that processes personal data on behalf of the College. A Data Subject is an individual whose personal data is collected or processed.

Data Collection & Use

The College collects and processes personal data only as necessary to support legitimate institutional functions and responsibilities. Individuals will be provided appropriate notice regarding the purpose of data collection when required, and the use of personal data will be limited to those purposes consistent with institutional operations, legal obligations, and regulatory requirements. The College will make reasonable efforts to maintain the accuracy of

personal data where practical and will retain such data only for the period necessary to meet legal, regulatory, operational, and records retention requirements.

Sensitive Data Protection

Sensitive personal data requires enhanced safeguards due to the potential risks associated with unauthorized disclosure or misuse. Access to sensitive personal data will be restricted to authorized personnel with a legitimate business need based on their job responsibilities. The College will implement appropriate protections such as encryption, secure transmission practices, monitoring controls, and additional access management safeguards where applicable. Sensitive personal data will not be disclosed without proper authorization unless disclosure is required by law.

Individual Rights Under OKDPA

Where applicable under the Oklahoma Data Privacy Act, individuals may have the right to confirm whether their personal data is being processed, request access to their personal data, request correction of inaccurate personal data, request deletion of personal data when appropriate, and opt out of certain categories of data processing. Requests related to these rights must be submitted to the designated institutional privacy contacts and will be reviewed and processed in accordance with institutional procedures and applicable legal requirements.

Data Security

The College will maintain reasonable administrative, technical, and physical safeguards designed to protect personal data against unauthorized access, accidental loss, misuse, alteration, or destruction. These safeguards are intended to support the integrity and availability of institutional systems and data resources while enabling the College to detect, respond to, and recover from security incidents. Employees are expected to follow institutional cybersecurity and data protection policies whenever handling personal data.

Third-Party Service Providers

Third-party service providers that process personal data on behalf of the College must enter into written agreements that clearly define their responsibilities related to data protection and security. These providers are required to maintain appropriate safeguards, use personal data only for authorized purposes consistent with contractual obligations, and promptly notify the College of any known or suspected data breaches involving institutional data. Vendor agreements must include appropriate privacy and security provisions consistent with OKDPA expectations and institutional standards.

Data Retention and Disposal

Personal data will be retained in accordance with institutional records retention schedules and applicable legal and regulatory requirements. When personal data is no longer required for institutional, legal, or operational purposes, it will be securely deleted or destroyed using approved disposal methods designed to prevent unauthorized access or reconstruction.

Data Breach Response

Any suspected or confirmed unauthorized disclosure, access, or misuse of personal data must be reported immediately to the Information Technology Department and appropriate institutional

leadership. The College will investigate incidents promptly and will comply with applicable breach notification requirements under Oklahoma law and other relevant regulations.

Compliance and Enforcement

Failure to comply with this policy may result in disciplinary action up to and including termination of employment or termination of contractual relationships. Violations may also result in civil or legal penalties under applicable law.